

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2000-260121

(P2000-260121A)

(43) 公開日 平成12年9月22日 (2000.9.22)

(51) Int.Cl.⁷

G 1 1 B 20/10

識別記号

3 0 1

F I

G 1 1 B 20/10

ターミナル (参考)

H 5 D 0 4 4

3 0 1 Z

審査請求 未請求 請求項の数 9 O L (全 25 頁)

(21) 出願番号

特願平11-58890

(22) 出願日

平成11年3月5日 (1999.3.5)

(71) 出願人 000003078

株式会社東芝

神奈川県川崎市幸区堀川町72番地

(72) 発明者 上林 達

神奈川県川崎市幸区小向東芝町1番地 株式会社東芝研究開発センター内

(72) 発明者 秋山 浩一郎

神奈川県川崎市幸区小向東芝町1番地 株式会社東芝研究開発センター内

(74) 代理人 100058479

弁理士 鈴江 武彦 (外6名)

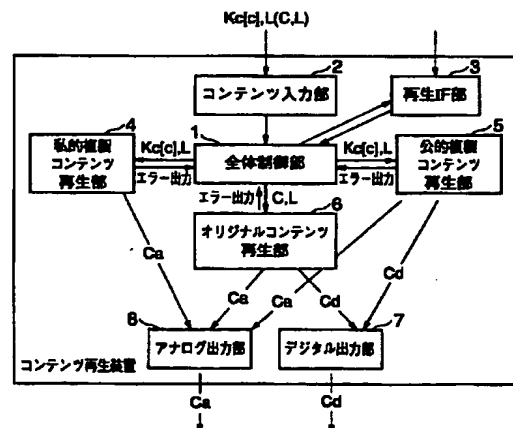
最終頁に続く

(54) 【発明の名称】 情報再生装置および情報記録装置

(57) 【要約】

【課題】 正当な経路で複製されたコンテンツ（公的複製コンテンツ）が、正当な権限なく複製されたコンテンツよりも有利な形態で流通可能となる。

【解決手段】 本発明の情報再生装置は、コンテンツ情報に付加された該コンテンツ情報を再生する際に必要なライセンス情報に基づき該コンテンツ情報を再生する情報再生装置において、暗号化されたコンテンツ情報を前記ライセンス情報の内容に基づき公的複製コンテンツ情報であるか私的複製コンテンツ情報であるかを判別する判別手段と、この判別手段で私的複製コンテンツ情報と判別されたコンテンツ情報は、公的複製コンテンツ情報よりも厳しい制限で再生する再生手段とを具備する。



【特許請求の範囲】

【請求項 1】 コンテンツ情報に付加された該コンテンツ情報を再生する際に必要なライセンス情報に基づき該コンテンツ情報を再生する情報再生装置において、暗号化されたコンテンツ情報を前記ライセンス情報の内容に基づき公的複製コンテンツ情報であるか私的複製コンテンツ情報であるかを判別する判別手段と、この判別手段で私的複製コンテンツ情報と判別されたコンテンツ情報は、公的複製コンテンツ情報よりも厳しい制限で再生する再生手段と、を具備したことを特徴とする情報再生装置。

【請求項 2】 前記ライセンス情報に含まれる公的複製であることを検証するための検証情報に基づき、公的複製コンテンツ情報であるか私的複製コンテンツ情報であることを判別することを特徴とする請求項 1 記載の情報再生装置。

【請求項 3】 前記ライセンス情報に含まれる前記コンテンツ情報の利用条件は、私的複製コンテンツ情報の方が公的複製コンテンツ情報よりも制限されていることを特徴とする請求項 1 記載の情報再生装置。

【請求項 4】 前記コンテンツ情報に付加されたライセンス情報は、該コンテンツ情報の記録されている記録媒体の識別子に依存する情報に基づき作成された鍵情報で暗号化および復号化されることを特徴とする請求項 1 記載の情報再生装置。

【請求項 5】 前記判別手段は、前記ライセンス情報の内容に基づき前記コンテンツ情報がオリジナルコンテンツ情報であるかを判別するものであり、オリジナルコンテンツ情報と判別されたときは、該コンテンツ情報を無制限に再生する第 2 の再生手段をさらに具備したことを特徴とする請求項 1 記載の情報再生装置。

【請求項 6】 コンテンツ情報と該コンテンツ情報に付加された該コンテンツ情報を再生する際に必要なライセンス情報とを記録媒体に記録する情報記録装置において、入力されたコンテンツ情報の種別を判別する判別手段と、この判別手段で判別された種別および前記記録媒体の識別子に依存する情報に基づき前記ライセンス情報を作成する作成手段と、この作成手段で作成されたライセンス情報とともに前記コンテンツ情報を前記記録媒体に記録する記録手段と、を具備したことを特徴とする情報記録装置。

【請求項 7】 コンテンツ情報と該コンテンツ情報に付加された該コンテンツ情報を再生する際に必要なライセンス情報とを記録媒体に記録する情報記録装置において、入力されたコンテンツ情報の種別を判別する判別手段と、この判別手段で判別された種別および前記記録媒体の識

別子に依存する情報および前記コンテンツ情報の利用条件に基づき前記ライセンス情報を作成する作成手段と、この作成手段で作成されたライセンス情報とともに前記コンテンツ情報を前記記録媒体に記録する記録手段と、を具備したことを特徴とする情報記録装置。

【請求項 8】 前記入力されたコンテンツ情報は、アナログ信号であることを特徴とする請求項 6 または請求項 7 記載の情報記録装置。

【請求項 9】 コンテンツ情報と該コンテンツ情報に付加された該コンテンツ情報を再生する際に必要なライセンス情報とを記録媒体に記録する情報記録装置において、前記記録媒体の識別子に依存する情報および前記コンテンツ情報の利用条件に基づき公的複製であることを検証するための検証情報を含む前記ライセンス情報を作成する作成手段と、この作成手段で作成されたライセンス情報とともに前記コンテンツ情報を前記記録媒体に記録する記録手段と、を具備したことを特徴とする情報記録装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は画像や音声等のコンテンツの記録再生装置に関する。

【0002】

【従来の技術】 CD プレーヤを始めとするデジタルコンテンツ再生装置は音質が綺麗な点、長時間の使用による音質劣化が少ないことなどから、多くの利用者があ

る。
【0003】 しかし、コンテンツがデジタルであるが 1 ビットずつオリジナルを忠実に複製することによって、劣化なくコピーすることが可能となっており、実際そのような機器が販売されている。そのようなコピー機器の存在はコンテンツ利用者にとっては大きなメリットではあるが、コンテンツ供給者からはコンテンツの販売に甚大な影響を与えるために好ましくはない。このためコンテンツ供給業者は新しいデジタル機器（及びメディア）が出た際はこれにコンテンツを供給しないことで対抗している。

【0004】 だが、この状況は、新しい電子機器の普及にあたって、大きな障害となり、その利便性を殆どの人が享受できないばかりかコンテンツ供給者もビジネスチャンスを失っている。

【0005】 また一方で、私的利用のための私的複製は著作権法でも認められた権利であり、実際現在までの多くの電子機器にあつては（アナログ記録への制限など）複製方式に制限はあるが認められてきた。だが、今後デジタルでの記録が主流になると私的複製と公的複製の区別が付きにくくなると同時に私的利用の判別が難しくなる。

【0006】 なお、ここでは、私的複製とは当該ソース

の販売権を持たない人によるコピーを言い、公的複製は当該ソースに販売権を持つ人によるコピーを言う。即ち、公的複製とは従来のコンテンツ販売と同等の手段でなければ取得できないものであり、インターネット上の電子商店からの販売も含まれる。

【0007】

【発明が解決しようとする課題】 以上の問題点に鑑み、本発明は、コンテンツが公的複製であるか私的複製であるによって当該コンテンツの再生方式を切り替え、公的複製の方が私的複製よりも有利な利用形態を許すことにより、正式な販路にのっている公的複製の需要を増やし、コンテンツ供給者、コンテンツ利用者、電子機器供給者に利害にかなった情報流通機構を構築できる情報再生装置、情報記録装置および情報販売装置および情報購入装置および情報自動販売機を提供することを目的とする。

【0008】

【課題を解決するための手段】 本発明では前記の課題を解決するため、暗号化コンテンツの利用を当該暗号化コンテンツに対応するライセンス情報によって制御すると同時に、公的複製である暗号化コンテンツに対応したライセンス情報にはコンテンツ販売が許可されているコンテンツ販売サーバだけが知っている公開鍵暗号方式の秘密鍵によって署名することにより、デジタル署名の有無によって公的複製と私的複製を判別し、判別結果に基づいて当該コンテンツの再生手段を変え、公的複製の方が私的複製よりも有利な再生手段で再生できる方式を実現する。

【0009】 (1) 本発明の情報再生装置は、コンテンツ情報に付加された該コンテンツ情報を再生する際に必要なライセンス情報に基づき該コンテンツ情報を再生する情報再生装置において、暗号化されたコンテンツ情報を前記ライセンス情報の内容に基づき公的複製コンテンツ情報であるか私的複製コンテンツ情報であるかを判別する判別手段と、この判別手段で私的複製コンテンツ情報と判別されたコンテンツ情報は、公的複製コンテンツ情報よりも厳しい制限で再生する再生手段とを具備する。

【0010】 また、前記ライセンス情報に含まれる公的複製であることを検証するための検証情報に基づき、公的複製コンテンツ情報であるか私的複製コンテンツ情報であるかを判別する。

【0011】 また、前記ライセンス情報に含まれる前記コンテンツ情報の利用条件は、私的複製コンテンツ情報の方が公的複製コンテンツ情報よりも制限されている。

【0012】 また、前記コンテンツ情報に付加されたライセンス情報は、該コンテンツ情報の記録されている記録媒体の識別子に依存する情報に基づき作成された鍵情報で暗号化および復号化される。

【0013】 また、前記判別手段は、前記ライセンス情

報の内容に基づき前記コンテンツ情報がオリジナルコンテンツ情報であるかを判別するものであり、オリジナルコンテンツ情報と判別されたときは、該コンテンツ情報を無制限に再生する第2の再生手段をさらに具備する。

【0014】 本発明の情報再生装置によれば、私的複製コンテンツと公的複製コンテンツやオリジナルコンテンツとの再生方法に構造上の差異を設け、私的複製を認めながら私的利用の拡大を防ぎ、著作権及びコンテンツ供給業者を保護している。

10 【0015】 また、コンテンツを別の記録媒体に不正に移す、即ちコピーした場合、ライセンス情報は、記録媒体に依存したものであるため、例えば、ライセンス情報が復号できなくなり、この結果としてコンテンツの復号ができなくなるため、私的複製であっても公的複製であっても、コピーのためにはライセンス情報を作り直さなければならない、それができるのは(例えば関数 f を知る)正当な記録装置だけであるためコピーの回数の制限などが確実にこなえることから不正利用を防止することができる。

20 【0016】 (2) 本発明の情報記録装置は、コンテンツ情報(暗号化されている場合と暗号化されていない場合とがある)と該コンテンツ情報に付加された該コンテンツ情報を再生する際に必要なライセンス情報(暗号化されたコンテンツ情報の復号鍵を含む場合もある)とを記録媒体に記録する情報記録装置において、入力されたコンテンツ情報の種別を判別する判別手段と、この判別手段で判別された種別および前記記録媒体の識別子に依存する情報に基づき前記ライセンス情報を作成する作成手段と、この作成手段で作成されたライセンス情報とともに前記コンテンツ情報を前記記録媒体に記録する記録手段とを具備している。

30 【0017】 本発明の情報記録装置は、コンテンツ情報(暗号化されている場合と暗号化されていない場合とがある)と該コンテンツ情報に付加された該コンテンツ情報を再生する際に必要なライセンス情報(暗号化されたコンテンツ情報の復号鍵を含む場合もある)とを記録媒体に記録する情報記録装置において、入力されたコンテンツ情報の種別を判別する判別手段と、この判別手段で判別された種別および前記記録媒体の識別子に依存する情報および前記コンテンツ情報の利用条件に基づき前記ライセンス情報を作成する作成手段と、この作成手段で作成されたライセンス情報とともに前記コンテンツ情報を前記記録媒体に記録する記録手段とを具備している。

40 【0018】 また、上記情報記録装置において、記録するコンテンツ情報は、アナログ信号に制限されてもよい。

50 【0019】 本発明の情報記録装置によれば、コンテンツの種類を判別して、ソースのコンテンツよりも厳しい制限でしか複製できないような環境を提供することにより、正式な販路に載った公的複製コンテンツと私的複製

コンテンツを差別化し、公的複製コンテンツの価値を相対的に上げることにより、公的複製コンテンツの販路の拡大に寄与する。

【0020】また、コンテンツを別メディアに不正に移す、即ちコピーした場合、ライセンス情報は、メディアに依存したものであるため、例えば、ライセンス情報が復号できなくなり、この結果としてコンテンツの復号ができなくなるため、私的複製であっても公的複製であっても、コピーのためにはライセンス情報を作り直さなければならず、それができるのは（例えば関数 f を知る）正当な記録装置だけであるためコピーの回数の制限などが確実にこなえることから不正利用を防止することができる。

【0021】また、記録されるソースコンテンツをアナログのみに限定することで、デジタルコンテンツを記録する際、複製を重ねる毎にコンテンツの質的劣化を引き起こすことができ、複製の抑止力となると同時に公的複製コンテンツの価値を相対的に上げ、公的複製コンテンツの販売市場を確保することがより確実にできる。

【0022】（3）本発明の情報記録装置は、コンテンツ情報と該コンテンツ情報に付加された該コンテンツ情報を再生する際に必要なライセンス情報とを記録媒体に記録する情報記録装置において、前記記録媒体の識別子に依存する情報および前記コンテンツ情報の利用条件に基づき公的複製であることを検証するための検証情報を含む前記ライセンス情報を作成する作成手段と、この作成手段で作成されたライセンス情報とともに前記コンテンツ情報を前記記録媒体に記録する記録手段とを具備している。

【0023】この情報記録装置は、特に、公的複製コンテンツを販売購入するためのコンテンツ販売装置、コンテンツ購入装置に用いることができる。

【0024】また、ライセンス情報は、記録媒体に依存したライセンス情報を作成するため、私的複製であっても公的複製であっても、コピーのためにはライセンス情報を作り直さなければならず、それができるのは（例えば関数 f を知る）正当な記録装置だけであるためコピーの回数の制限などが確実にこなえることから不正利用を防止することができる。

【0025】

【発明の実施の形態】以下、本発明の実施形態について、図面を参照して説明する。

【0026】まず、以下の説明で用いる用語について説明する。

【0027】ライセンス情報は、コンテンツ自体に埋め込まれるものと、暗号化コンテンツに付加情報として関連付けられる外部情報とがある。ここで前者は電子透かしの手法でアナログレイヤで実現され、ここではアナログライセンス情報と呼ぶことにする。後者は、デジタルレイヤで実現されるので、デジタルライセンス情報と呼

ぶ。さらに、両者を併せてライセンス情報という。

【0028】本発明のコンテンツ記録再生装置に入力されるコンテンツは3種類あり、オリジナルコンテンツ、公的複製コンテンツ、私的複製コンテンツである。

【0029】オリジナルコンテンツは自作のコンテンツか、コピーフリーで特定の利用制限がないコンテンツである。このためオリジナルコンテンツは暗号化されていないし、後述するライセンスヘッダのみのデジタルライセンス情報が付加されているものとする。

10 【0030】公的複製コンテンツとは当該コンテンツの販売権を持つ者によって複製されたコンテンツをいう。公的複製コンテンツはコンテンツが暗号化されていると同時に販売権を証明するデジタル署名が付加されたデジタルライセンス情報が付けられている。

【0031】私的複製コンテンツとは当該コンテンツの販売権を持たない者によって複製されたコンテンツをいう。私的複製コンテンツはコンテンツが暗号化されていると同時にデジタル署名が付加されていないデジタルライセンス情報が付けられている。

20 【0032】次に、デジタルライセンス情報の具体的な構造について説明する。デジタルライセンス情報 L_o は、図1に示すようにライセンスヘッダ(LH)、コンテンツ鍵(Kc)、コンテンツ利用条件(U)、認証子(MAC)、デジタル署名からなっている。

【0033】ライセンスヘッダは、図3に示すようにライセンス情報の長さ、コンテンツの識別子(ID)、複製情報、コンテンツ鍵の長さからなっている固定長のデータである。ライセンス情報の長さはライセンス情報の全体長を示しており、ライセンス抽出時に利用する。複製情報は、当該コンテンツがオリジナルコンテンツか、公的複製コンテンツか、私的複製コンテンツかを区別するための情報である。コンテンツ鍵の長さはライセンス情報に含まれるコンテンツ鍵の長さを示す。

【0034】デジタルライセンス情報中のコンテンツ利用条件Uは、当該デジタルライセンス情報に対応しているコンテンツの利用条件を示しており、図4に示すような構成をしている。図4において、デジタル出力フラグFeは「1」のとき、当該コンテンツのデジタル出力を許可し、「0」のときは許可しない。有効期限情報は当該コンテンツの有効期限を示している。同様に有効回数

40 は当該コンテンツが利用できる回数を指定している。これらは全てシステムによって定められた固定長のデータである。

【0035】なお、ここで示したデジタルライセンス情報はほんの一例であって、応用形態によって様々に変更される。

50 【0036】認証子はデジタルライセンス情報に含まれるコンテンツ鍵やコンテンツ利用条件が正しいものであるかチェックするためのデータであって、誤り検出と改竄防止の効果を持っている。

【0037】デジタル署名は、図6に示すように、デジタル署名ヘッダとデジタル署名とからなる。なお、デジタル署名ヘッダは、図7に示すように、デジタル署名の全体長（ビット長）と、当該デジタル署名の種類と署名検証鍵番号とからなっている。

【0038】デジタルライセンス情報L_oにはコンテンツ鍵K_cが含まれているので暗号化されなくてはならない。しかし一方で、デジタルライセンス情報を全て暗号化してしまうと、複製情報を取得するだけの目的でも復号しなくてはならなくなったり、オリジナルコンテンツのように本来暗号化の必要のないものまで暗号化する必要が生じる。これを避けるため本実施形態では、図2に示すように、暗号化の範囲をコンテンツ鍵、コンテンツ利用条件、認証子の部分に限る構成を示している。図2にも示されているように、以下では、情報Iを鍵Kで暗号化したデータをI[K]もしくは[K]Iと表すことにする。また、デジタルライセンス情報およびコンテンツの暗号化には共通鍵暗号を使うことを前提としている。共通鍵暗号は暗号鍵と復号鍵とが一致している暗号方式である。以下の実施形態においては文脈上、復号鍵で暗号化したり、暗号鍵で復号したりする記述があるが、これは前記の理由により矛盾するものではない。

【0039】暗号化デジタルライセンス情報は図2のような構造をしており、ライセンスヘッダとデジタル署名を除く部分を後に詳しく述べるライセンス鍵で暗号化する。

【0040】次に、アナログライセンス情報に関して説明する。アナログライセンス情報は、電子透かしとしてコンテンツ自体に埋め込まれるものであって、再生されたアナログコンテンツに埋め込まれているので、暗号によるコンテンツの著作権保護が破れても尚有効である。だが一方で、コンテンツ自体に情報を埋め込むので、埋め込みに時間がかかるという欠点がある。

【0041】そこで、本実施形態では、アナログライセンス情報として図5に示すような構造を考える。即ち、アナログライセンス情報Iは、コピー回数制限情報と複製情報からなり、コピー回数制限情報は当該コンテンツのコピー回数の（無制限を含む）上限値を表わし、複製情報は図3のライセンスヘッダL_Hに含まれる複製情報と同じ情報が入る。

【0042】（第1の実施形態）第1の実施形態では、入力されたコンテンツがオリジナルコンテンツ、私的複製コンテンツ、公的複製コンテンツであるかをライセンス情報を基に判別し、それに伴ってコンテンツの再生方式を変えるコンテンツ再生装置について説明する。

【0043】本実施形態に係るコンテンツ再生装置の全体構成図を図8に、処理の流れを図12のフローチャートに示している。以下、図12のフローチャートを参照しながら図8のコンテンツ再生装置について説明する。

【0044】まず、再生I/F部3からの再生指示によ

り、コンテンツ入力部2にコンテンツCと暗号化デジタルライセンス情報Lを入力する（ステップS1）。これらの情報は全体制御部1に送られ、ここで暗号化デジタルライセンス情報のライセンスヘッダを参照して、当該コンテンツがオリジナルコンテンツか、私的複製コンテンツか、公的複製コンテンツかを識別し（ステップS2～ステップS4）、その識別結果に応じて、それぞれ、オリジナルコンテンツの再生処理、私的複製コンテンツの再生処理、公的複製コンテンツの再生処理を行なう（ステップS6～ステップS8）。

【0045】これら3種類のコンテンツに該当しないものは、本発明のコンテンツ再生装置において解釈ができないコンテンツであるので、エラー出力を行ない、処理を終了する（ステップS5）。

【0046】3つの種類に応じたコンテンツ毎の再生処理は図8のそれぞれの再生部において行なわれる。これらの具体的な構成と処理の流れに関しては後述するが、私的複製コンテンツ再生部4からデジタル出力部7へコンテンツが流れないような構成を取る点は重要である。即ち、私的複製コンテンツは私的利用の目的のみに再生が許可されたものであり、コンテンツの一部を切り貼りするなどの2次利用に関しては私的利用の範囲を逸脱する可能性が高く、コンテンツ供給業者としては許可し難い。本発明では、この点に鑑み、私的複製コンテンツと公的複製コンテンツやオリジナルコンテンツとの再生方法に構造上の差異を設け、私的複製を認めながら私的利用の拡大を防ぎ、著作権及びコンテンツ供給業者を保護している。

【0047】図8のオリジナルコンテンツ再生部6の構成図を図9に、その処理の流れを図13に示す。オリジナルコンテンツは前述したように、暗号化されていないコンテンツを言う。ライセンス情報に関しては、本実施形態においては、デジタルライセンス情報はライセンスヘッダのみ、アナログライセンス情報に関してはコピー回数を無制限で設定されているものとする。

【0048】以下、図13のフローチャートを参照しながら図9のオリジナルコンテンツの再生部6について説明する。

【0049】オリジナルコンテンツは、コンテンツ入力部6cに入力し（ステップS21）、データ解凍部6fでMPEGなどの圧縮形式が解凍されて（ステップS22）、その結果出力されるデジタルコンテンツCに関してD/A変換部6gにてデジタル信号からアナログ信号に変換（D/A変換）する（ステップS23）。そして、アナログライセンス情報検出部6dにて、コンテンツに埋め込まれたアナログライセンス情報を検出したら（ステップS24）、制御部6aは、その中の複製情報を参照することにより、当該コンテンツがオリジナルコンテンツであるかどうかを判別する（ステップS25）。もし、オリジナルコンテンツでなければその時点

でエラーを出力して終了する(ステップS29)。オリジナルコンテンツであれば、デジタル出力の指示が来ている場合は(ステップS26)、デジタル出力部6eを介してデジタル出力を(ステップS30)、そうでない場合は、デジタルコンテンツCをD/A変換部6gでデジタル信号からアナログ信号に変換し、アナログ出力部6hを介して出力する(ステップS27～ステップS28)。

【0050】図8の私的複製コンテンツ再生部4の構成図を図10に、その処理の流れを図14に示す。私的複製コンテンツは前述したように、暗号化されており、デジタルライセンス情報に(公的複製であることを証明する)デジタル署名がないコンテンツを言う。

【0051】以下、図14のフローチャートを参照しながら図10の私的複製コンテンツ再生部4について説明する。

【0052】私的複製コンテンツは、暗号化デジタルライセンス情報Lとともに、暗号コンテンツ入力部4bに入力する(ステップS31)。これらの情報は暗号化コンテンツ復号部4cに送られ、ここで後に詳しく述べる処理によって暗号化デジタルライセンス情報を復号し(ステップS32)、デジタルライセンス情報に含まれるコンテンツ鍵Kcを用いて暗号化コンテンツを復号する。また、デジタルライセンス情報から利用条件Uを抽出する(ステップS33～ステップS35)。

【0053】制御部4aは、利用条件Uをチェックし(ステップS36)、利用不可能と判定された場合はエラーを出力して終了する(ステップS42)。利用可能であった場合、更に、利用条件に記載されている条件が私的複製コンテンツに許可されている範囲(上限値)を逸脱しているか否かをチェックする。ここで逸脱している場合は当該条件を上限値に設定した上でステップS37へ進む。このようにすることによって、ライセンス情報の偽造などにシステムとして対応できる。

【0054】制御部4aは、復号されたコンテンツCをデータ解凍部4dへ送り、MPEGなどの圧縮形式を解凍し、デジタルコンテンツCdを出力する(ステップS37)。デジタルコンテンツCdに対してD/A変換部4eにてデジタル信号からアナログ信号に変換した後(ステップS38)、アナログライセンス情報検出部4fはコンテンツに埋め込まれたアナログライセンス情報を検出する(ステップS39)。そして、制御部4aは、アナログライセンス情報の中の複製情報を参照することにより、当該コンテンツが私的複製コンテンツであるかどうかを判別する(ステップS40)。もし、私的複製コンテンツでなければその時点でエラーを出力して終了する(ステップS43)。私的複製コンテンツであれば、D/A変換部4eでD/A変換し、アナログ出力部4gを介してアナログ出力を行なう(ステップS41)。なお、ここでデジタル出力の指示が来てもデ

ジタル出力は行なわない。

【0055】図8の公的複製コンテンツ再生部5の構成図を図11に、その処理の流れを図15に示す。公的複製コンテンツは前述したように、暗号化されており、デジタルライセンス情報に(公的複製であることを証明する)デジタル署名が付加されているコンテンツを言う。

【0056】以下、図15のフローチャートを参照しながら図11の公的複製コンテンツ再生部5について説明する。

10 【0057】公的複製コンテンツは、暗号コンテンツ入力部5bに暗号化デジタルライセンス情報とともに入力される(ステップS51)。これらの情報は暗号化コンテンツ復号部5cに送られ、ここで後に詳しく述べる処理によって暗号化デジタルライセンス情報にデジタル署名が付加されているかを検証し、付加されている場合は、デジタル署名検証鍵を用いてデジタル署名を検証することによって公的複製であることを検証する(ステップS52～ステップS53)。なお、ステップS52でデジタル署名が付加していなかった場合、ステップS53でデジタル署名が検証できなかった場合はエラーを出力し処理を終了する(ステップS64～ステップS65)。

【0058】ステップS53でデジタル署名が検証できた場合は、後に詳しく述べる処理によって暗号化デジタルライセンス情報を復号し(ステップS54)、デジタルライセンス情報に含まれるコンテンツ鍵Kcを用いて暗号化コンテンツを復号する。また、デジタルライセンス情報から利用条件Uを抽出する(ステップS55～ステップS57)。

30 【0059】制御部5aは、利用条件をチェックし(ステップS58)、利用不可能と判定された場合はエラーを出力して終了する(ステップS66)。利用可能であった場合、更に、利用条件に記載されている条件が私的複製コンテンツに許可されている範囲(上限値)を逸脱しているか否かをチェックする。ここで逸脱している場合は当該条件を上限値に設定した上でステップS59へ進む。このようにすることによって、ライセンス情報の偽造などにシステムとして対応できる。

40 【0060】制御部5aは、復号されたコンテンツCをデータ解凍部5dへ送り、MPEGなどの圧縮形式を解凍し、デジタルコンテンツCdを出力する(ステップS59)。デジタルコンテンツCdに対してD/A変換部5eでD/A変換を行った後(ステップS60)、アナログライセンス情報検出部5fは、コンテンツに埋め込まれたアナログライセンスを検出する。そして、制御部5aは、アナログライセンス情報の中の複製情報を参照することにより、当該コンテンツが公的複製コンテンツであるかどうかを判別する(ステップS61)。もし、公的複製コンテンツでなければその時点でエラーを出力して終了する(ステップS67)。公的複製コンテンツ

であれば、デジタル出力の指示が来ている場合は（ステップS62）デジタル出力部5iを介してデジタル出力を（ステップS68）、そうでない場合はD/A変換部5eでD/A変換し、アナログ出力部5gを介してアナログ出力を行なう（ステップS63）。

【0061】次に、暗号化コンテンツ復号部について説明する。この構成部は、私的複製コンテンツ再生部4、公的複製コンテンツ再生部5に存在し、どちらも構成は類似している。まず、公的複製コンテンツ再生部5の暗号化コンテンツ復号部5cについて述べ、私的複製コンテンツ再生部4の暗号化コンテンツ復号部4cに関しては暗号化コンテンツ復号部5cとの差異のみを述べることにする。

【0062】暗号化コンテンツ復号部5cの構成例を図16に、その処理の流れを図18に示す。以下、図18のフローチャートを参照して暗号化コンテンツ復号部5cについて説明する。

【0063】暗号化コンテンツKc [C] と暗号化デジタルライセンス情報Lとが暗号化ライセンス復号部5cに入力すると（ステップS71）、暗号化ライセンス復号部5cでは、メディアID抽出部（公的複製コンテンツ再生部5の場合は、メディアID抽出部5h、私的複製コンテンツ再生部4の場合は、メディアID抽出部4h）を通じて当該コンテンツの記録されていたメディアMの識別子であるメディアIDを取得する（ステップS72）。そのメディアIDを用いて、後に詳しく述べる手段により、ライセンス復号鍵wを作成し、復号されたデジタルライセンス情報を出力する（ステップS73）。

【0064】図1に示すデジタルライセンス情報のうち、コンテンツ鍵Kcとコンテンツ利用条件Uから認証子を計算する（ステップS75）。認証子は、例えばコンテンツ鍵とコンテンツ利用条件を連結した情報を一方方向関数の入力として出力された値とする。

【0065】ここでの認証子の役割は、ライセンス鍵wが間違っているために間違ったコンテンツ復号鍵や利用条件が出力されることがないようにする誤り検出の役割である。MACの生成は一方方向関数によって実現される。一方方向関数はハッシュ関数や暗号関数によっても実現され、出力値から入力値が推定できないような関数をいう。

【0066】MAC照合部102は、暗号化ライセンス復号部101からの出力から計算された認証子と、同じく暗号化ライセンス復号部101から出力された図1のデジタルライセンス情報にもともと含まれている認証子MACとを照合して（ステップS76）、一致すれば出力されたコンテンツ復号鍵Kcは信頼できるので（ステップS77）、このKcを用いて、コンテンツ復号部103にて、暗号化コンテンツを復号する（ステップS78）。認証子が一致しなかった場合は、エラー出力し処

理を終える（ステップS81）。

【0067】認証子を照合し、暗号化コンテンツが復号できた場合、コンテンツCと利用条件Uを出力し、暗号化コンテンツ復号部の処理を終了する（ステップS79）。

【0068】次に、暗号化コンテンツ復号部の構成要素である暗号化ライセンス復号部101について詳しく説明する。構成を図17に、その処理の流れを図19に示す。

10 【0069】以下、図19に示すフローチャートを参照して、暗号化ライセンス復号部101について説明する。

【0070】暗号化デジタルライセンス情報Lが入力すると（ステップS91）、まずデジタル署名検出部101aにおいてデジタル署名の検出が行なわれる（ステップS92）。すなわち、デジタル署名の検出はライセンスヘッダ中のデータを用い、例えば、次式を用いてデジタル署名の先頭アドレスを算出する。

20 【0071】デジタル署名の先頭アドレス＝暗号化デジタルライセンス情報の先頭アドレス＋（ライセンスヘッダ長＋コンテンツ鍵の長さ＋コンテンツ利用条件の長さ＋認証子の長さ）

デジタル署名検証鍵取得部101bは、このデジタル署名の先頭アドレスから固定長のデジタル署名ヘッダを取得し（図6、図7参照）、そこに記載されているデジタル署名の全体長、署名の種類、署名検証鍵の番号から署名アルゴリズム及びその検証鍵を特定することができる。署名の種類、署名検証鍵の番号が取得できたら、それをもとに、デジタル署名検証鍵保持部101fを検索し、当該署名の種類、署名検証鍵の番号に対応する署名アルゴリズム、検証鍵を取得する（ステップS94）。

【0072】デジタル署名（ヘッダ）が検出できなかった場合は、エラー出力して処理を終了する（ステップS93、ステップS101）。

【0073】デジタル署名が検出できたら、次に、デジタル署名検証部101cは、検出されたデジタル署名を、デジタル署名ヘッダにて指定された署名アルゴリズムと署名検証鍵番号の署名検証鍵を使って検証する（ステップS95）。

40 【0074】ここでのデジタル署名は公開鍵暗号によるそれを考えている。即ち、署名作成鍵（秘密鍵）を持っている認可されたサーバもしくは販売店のみが、公的複製コンテンツに対応するライセンスファイルが作成できる。それ以外の者は例え再生装置を所有していても、その中にあるのは署名検証鍵（公開鍵）だけであり、公開鍵から秘密鍵を求めることが難しいのが公開鍵暗号の安全性であるので、充分安全な公開鍵暗号を使えば、秘密鍵を知らない第三者はライセンスに対応したデジタル署名は作成できないことになる。このことから公的複製コンテンツに対応したライセンスが作れるのは認可された

販売者であることが導かれる。しかし一方で、公開鍵暗号も攻撃法（解読法）の発展によりいつまでも安全であるとは限らない。この点に鑑みて、デジタル署名のヘッダの中で署名アルゴリズム、署名検証鍵を指定して随時サーバ側で変更できるような構成となっている。

【0075】デジタル署名検証部101cで署名検証結果がNGと判断された場合はエラー出力する（ステップS96、ステップS102）。そうでない場合は、ライセンス鍵生成部101dは、暗号化コンテンツが記録されているメディアのメディアID（MID）を取得し（ステップS97）、これを再生装置の中に秘密に保持された関数を用いて、 $w = f(MID)$ からメディアに依存したライセンス鍵wを得る（ステップS98）。

【0076】これはコンテンツを別メディアに移す、即ちコピーした場合、メディアに依存したライセンス鍵wしか得られないため、暗号化デジタルライセンス情報が復号できなくなり、この結果としてコンテンツの復号ができないようにするための仕組みである。

【0077】このように私的複製であっても公的複製であっても、コピーのためには暗号化デジタルライセンス情報を作り直さなければならず、それができるのは関数fを知る正当な記録装置だけであるためコピーの回数の制限などが確実にこなえることから不正利用を防止することができる。この意味から、関数fを実現するハードウェアもしくはファームウェアは耐タンパなLSIの中に存在することが望ましい。

【0078】ライセンス復号部101eは、このようにして作成されたライセンス鍵wを用いて暗号化デジタルライセンス情報を復号し（ステップS99）、デジタルライセンス情報Loを得、それを出力する（ステップS100）。

【0079】以上が、公的複製コンテンツ再生部5の暗号化コンテンツ復号部5cおよびその構成要素である暗号化ライセンス復号部101の説明である。尚、私的複製コンテンツ再生部4の暗号化コンテンツ復号部4cの暗号化ライセンス復号部101は、図17のデジタル署名検出部101c、デジタル署名検証鍵取得部101b、デジタル署名検証鍵保持部101f、デジタル署名検証部101cは構成として必ずしも必要ではなく、それらの処理は不要である。

【0080】次に、以上説明したコンテンツ再生装置についてのいくつかのバリエーションを述べる。

【0081】まず、図8の全体構成において、コンテンツの種類によって再生部を完全に分離した形を示しているが、これは必ずしも必要ではない。実質上はライセンスファイルの種類によって別れ、更に前述したように処理も似ている部分も多い。このことから、同一の処理をする部分を一つの回路にすることにより、回路規模を小

さくすることができる。また、逆に同じ機能を持った回路であっても仕様を再生部毎に変更しておくことで、安全性を向上させることができる。例えば、各再生部のデータ解凍部（4d、5d、6f）では、コンテンツの種類毎に別々のアルゴリズムを使うことで、ライセンス情報によってコンテンツの種類を偽ることがより難しくなる。

【0082】また、オリジナルコンテンツ再生部を持たない再生装置の構成も考えられる。この場合、再生装置の側でオリジナルコンテンツの再生はできなくなり、コンテンツは公的複製コンテンツと私的複製コンテンツの2つに限られることになる。このようにすることによって、自作のコンテンツでも私的複製コンテンツとして見なされるという問題点があるが、その反面、ラジオやテレビからのコンテンツのダビングなど自作コンテンツでないものをオリジナルコンテンツとして記録し無条件に再生されてしまうという問題は避けられる。

【0083】更にデジタル署名に関しては、図1の形態で付加する以外にも、図20に示すように、ライセンス鍵wでの暗号化の上からさらに署名生成鍵Ksで再暗号化を行っても良い。このようにしても、異なった署名生成鍵で暗号化しても、正しい署名検証鍵で復号しても正しく復号できないように構成することができる。正しく復号できたかどうかの判定は認証子MACによって確実に判定できる。このようにすることによってデジタル署名分のデータサイズが削減できる。

【0084】（第2の実施形態）ここでは、自作のコンテンツからオリジナルコンテンツもしくは私的複製コンテンツ、公的複製コンテンツからは私的複製コンテンツを製作することができるコンテンツ記録装置について説明する。

【0085】本実施形態は、前述した第1の実施形態の再生装置に対応した記録装置であり、当該再生装置と一体化し、コンテンツ記録再生装置を構成することができる。

【0086】本実施形態に係るコンテンツ記録装置の全体構成を図21に、その処理の流れを図24のフローチャートに示している。以下、図24のフローチャートを参照しながら図21のコンテンツ再生装置について説明する。

【0087】コンテンツ入力部202には、コンテンツとして暗号化されたコンテンツ（Kc[C]）もしくは暗号化されていないコンテンツCが暗号化ライセンス情報Lとともに入力される（ステップS201）。

【0088】全体制御部201は、暗号化デジタルライセンス情報のライセンスヘッダを参照して、当該コンテンツが公的複製コンテンツであれば（ステップS202）、私的複製コンテンツ作成部204にこれらのデータを送り、私的複製コンテンツ作成処理に進む（ステップS203）。

【0089】当該コンテンツが私的複製コンテンツであれば（ステップS204）、私的複製コンテンツ作成部204にこれらのデータを送り、私的複製コンテンツ作成処理に進む（ステップS205）。

【0090】当該コンテンツがオリジナルコンテンツであれば（ステップS206）、オリジナルコンテンツ作成部205にこれらのデータを送り、オリジナルコンテンツ作成処理を開始する（ステップS207）。

【0091】このようにコンテンツの種類により記録手段を変更し、記録装置では高々私的複製しかできないような環境を提供することにより、正式な販路に載った公的複製コンテンツと私的複製コンテンツを差別化し、公的複製コンテンツの価値を相対的に上げることに、公的複製コンテンツの販路の拡大に寄与する。

【0092】次に、図21のコンテンツ記録装置の私的複製コンテンツ作成部204に関して詳しく説明する。図22に私的複製コンテンツ作成部204の構成例を、その処理の流れを図25～図26に示す。

【0093】以下、図25～図26に示すフローチャートを参照して、私的複製コンテンツ作成部204について説明する。

【0094】私的複製コンテンツを複製する際、まず、コンテンツ入力部204bから暗号化コンテンツKc[C]と、その暗号化デジタルライセンス情報Lと、複製形態情報Qが入力され、処理が開始される（ステップS211）。

【0095】複製形態情報Qとは図30に示す構造をしている。すなわち、複製形態情報Qは複製後のコンテンツ種別（複製コンテンツ種別）と、複製コンテンツの利用条件（利用条件情報）とが記載されている。

【0096】ここで、利用条件情報は、図31に示す構成をしており、デジタル出力フラグ、有効期限情報、有効利用回数情報、コピー回数制限情報からなり、それぞれデジタルライセンス情報、アナログライセンス情報に記載されている情報に埋め込むための情報である。

【0097】なお、以下の処理でも明らかになるように、複製後のコンテンツ種別により、必ずしもこれらの情報がそのまま反映される訳ではない。後にも説明するようにこれは複製後のコンテンツ種別により、各上限値が規定されており、この上限値を越えて設定することを許さないためである。このことにより私的複製コンテンツ、公的複製コンテンツ、オリジナルコンテンツに利用上の区別を付け、コンテンツ供給業者の利益にかなったシステムを実現する。

【0098】さて、入力された暗号化コンテンツKc[C]と、その暗号化デジタルライセンス情報Lと、複製形態情報Qとは、制御部204aに送られ、暗号化コンテンツKc[L]と暗号化デジタルライセンス情報Lはコンテンツ復号部204eに送られる。

【0099】コンテンツ復号部204eでは、第1の実

施形態のコンテンツ再生装置のコンテンツ再生と同様に、暗号化コンテンツを復号する。すなわち、ソース側のメディアMからメディアID取得部206を経由してメディアID(MID)を取得し（ステップS212）、当該メディアIDと秘匿された関数fとを用いて、

$w = f(MID)$

という関係式からライセンス鍵wを作り（ステップS213）、暗号化デジタルライセンス情報Lを復号する（ステップS214）。復号されたデジタルライセンス情報からコンテンツ復号鍵Kcを抽出する（ステップS215）。さらに、デジタルライセンス情報から認証子を抽出し、これを検査することによってコンテンツ復号鍵Kcに誤りがないことを確認する（ステップS216）。そして、コンテンツ復号鍵Kcを用いて暗号化コンテンツを復号し、コンテンツCを得る（ステップS218）。

【0100】コンテンツ復号部204eで復号されたコンテンツCは、制御部204aを経由してアナログライセンス検出・修正部204fに送られる。ここでは、まず、データ解凍部204gにコンテンツCを送り、コンテンツCの圧縮を解凍し（ステップS219）、解凍されたデジタルコンテンツCに対して、D/A変換を行ない（ステップS220）、アナログコンテンツCaを得る。このアナログコンテンツCaからアナログライセンス情報を抽出し（ステップS221）、アナログライセンス情報の複製情報により、当該コンテンツの種類を特定する。

【0101】当該ソースのコンテンツが公的複製コンテンツであった場合（ステップS222）、図5に示すようなアナログライセンス情報の複製情報を私的複製コンテンツと修正し（ステップS226）、同じくアナログライセンス情報のコピー回数制限情報を私的複製コンテンツに許された上限値に設定する（ステップS227）。

【0102】一方、当該ソースのコンテンツが私的複製コンテンツの場合は（ステップS223）、図5に示すようなアナログライセンス情報のコピー回数制限情報を「1」減算する（ステップS224）。

【0103】また、当該ソースのコンテンツが公的複製コンテンツでも私的複製コンテンツでもない場合、エラー出力をする（ステップS228）。

【0104】以上の処理で作成されたアナログライセンス情報を現在記録されているアナログライセンス情報を消去して、アナログコンテンツに埋め込む（ステップS225）。さらに、A/D変換してデジタルコンテンツCdに変換した後（ステップS229）、データ圧縮部204hに送り圧縮処理を行なって（ステップS230）、新しいコンテンツCを得る。

【0105】新しいコンテンツCは、アナログライセン

ス情報検出・修正部204fから制御部204aを経由して、コンテンツ暗号化部204dへコンテンツ暗号鍵Kcとともに送られる。

【0106】コンテンツ暗号化部204dでは、入力されたコンテンツCを同じく入力されたコンテンツ復号鍵Kcで暗号化し、暗号化コンテンツKc[C]を得る(ステップS231)。

【0107】一方、制御部204aでは、複製形態情報Qの利用条件情報に記載されているデジタル出力フラグ、有効期限情報、有効利用回数制限を参照し、これらの条件が私的複製コンテンツの範囲を逸脱していないことを確認する。逸脱していた場合は私的複製コンテンツにおいて認められている範囲でデジタルライセンス情報に含まれるコンテンツ利用条件Uを作成する(ステップS232)。

【0108】次に、コンテンツ復号鍵Kcとコンテンツ利用条件Uとから認証子(MAC)を計算する(ステップS233)。計算の方式は前述した第1の実施形態のコンテンツ再生装置で認証子確認のために行なった計算と同じである。

【0109】さらに、ライセンスヘッダの複製情報の部分に私的複製コンテンツである旨の情報その他を算出して格納し、当該コンテンツのデジタルライセンス情報が完成する。

【0110】次に、デジタルライセンス情報の暗号化のためターゲット側(記録側)メディアM'からメディアID取得部206を通じてメディアID(MID)を取得する(ステップS235)。取得されたメディアID(MID)から

$w = f(MID)$

によってライセンス鍵wを生成する(ステップS236)。この生成方式は前述したコンテンツ復号部204eの処理の部分で述べた暗号化デジタルライセンス情報Lの際に作成したライセンス鍵の作成方式と同じである。だが前者の場合とはMIDが異なるので異なるライセンス鍵が生成される。

【0111】このように複製の前後で暗号化デジタルライセンス情報のデータを変更することで、不正な複製を防ぐことができるのである。

【0112】ステップS236で得られたライセンス鍵wを使ってデジタルライセンス情報Loを暗号化して暗号化デジタルライセンス情報Lを得る(ステップS237)。

【0113】以上によって記録すべきデータは全て完成し、暗号化コンテンツKc[C]と暗号化デジタルライセンス情報Lとをそれぞれコンテンツ記録部208、ライセンス記録部207を通じてターゲット側メディアM'に記録する(ステップS238～ステップS239)。

【0114】次に、図21のコンテンツ記録装置の中の

オリジナルコンテンツ作成部205に関して詳しく説明する。オリジナルコンテンツ作成部205の構成を図23に、その処理の流れを図27～図29に示す。

【0115】以下、図27～図29に示すフローチャートを参照して、図23のオリジナルコンテンツ作成部205について説明する。

【0116】オリジナルコンテンツを複製する際、まず、コンテンツ入力部205bからコンテンツCと複製形態情報Qが入力され、処理が開始される(ステップS241)。

【0117】コンテンツCが制御部205aを経由して、アナログライセンス情報検出修正部205dに送られ、ここからデータ解凍部205gの処理によりコンテンツの解凍が行なわれる(ステップS242)。

【0118】解凍されたデジタルコンテンツCdにD/A変換を施し、アナログライセンス情報を検出する(ステップS243～S244)。ここでオリジナルコンテンツであれば検出されないはずであるが、データの一部を改竄することにより、当該コンテンツをオリジナルコンテンツになりすまして入力していた場合などはここでエラー出力し、処理を終了する(ステップS245～ステップS246)。

【0119】オリジナルコンテンツであった場合、次に複製先をオリジナルコンテンツとするのか私的複製コンテンツとするのかを複製形態情報Qの複製コンテンツ種別によって判断する(ステップS247)。

【0120】オリジナルコンテンツは、先に定義したように利用者自身に著作権のあるコンテンツを考えているので暗号化しないオリジナルコンテンツにも私的複製コンテンツにも複製できる。当然オリジナルコンテンツに複製した方がより有利な条件で再生できるが、著作者自身が複製先で利用形態に何らかの制限を設けたい場合は私的複製コンテンツとして記録することによって目的は実現される。

【0121】私的複製コンテンツとして複製したい場合は、ステップS248へ進み、アナログライセンス情報をコンテンツに記録する必要がある。このためアナログライセンス情報を作成し、その複製情報を私的複製とし、コピー回数制限を利用形態情報Qに含まれるコピー回数制限情報を私的複製コンテンツで許可されているコピー回数の上限値を越えない範囲で設定し、当該アナログライセンス情報をコンテンツCに埋め込み、A/D変換し、更に、データ圧縮部205hで圧縮処理を施すことにより新たなコンテンツCを得る(ステップS248～ステップS252)。

【0122】一方、オリジナルコンテンツとして複製する場合には、ステップS247からステップS251へ進み、アナログライセンス情報の修正処理をすることなしにA/D変換を行ない、圧縮処理を行なってコンテンツCを得る(ステップS251～ステップS252)。

【0123】以上の処理で作成されたコンテンツCはアナログライセンス情報検出修正部205dから制御部205aへ送られ、制御部205aで複製形態情報Qを参照して私的複製コンテンツに複製するか、オリジナルコンテンツに複製するかによって処理手順を変える(ステップS253)。

【0124】まず、オリジナルコンテンツに複製する場合は、暗号化する必要がないので、ライセンス生成部205cは、デジタルライセンス情報をライセンスヘッダのみ作成し、ライセンスヘッダ中の複製情報を「オリジナルコンテンツ」とし(ステップS264)、ライセンス記録部207を通じて当該デジタルライセンス情報をターゲット側のメディアに記録する(ステップS262)。ここでオリジナルコンテンツの場合のデジタルライセンス情報はライセンスヘッダのみ存在するため暗号化部分はなく、ライセンス鍵も作成しなくても良い。また、コンテンツCも暗号化する必要がないのでそのままコンテンツ記録部208を通し、ターゲット側のメディアに記録される(ステップS263)。

【0125】次に、私的複製コンテンツとして記録する場合の処理に関して述べる。私的複製コンテンツとして記録する場合は(ステップS253)、コンテンツCを暗号化し、しかも当該コンテンツに対応したコンテンツ復号鍵Kcが含まれる暗号化デジタルライセンス情報Lを作成し、メディアに記録しなくてはならない。順次その手順を説明する。

【0126】制御部205aは、コンテンツCをコンテンツ暗号化部205eに送り、コンテンツ暗号化部205eでは、コンテンツ復号鍵生成部205fに命令を出し、コンテンツ鍵Kcを作成させる(ステップS254)。作成されたコンテンツ復号鍵KcでコンテンツCを暗号化し(ステップS255)、暗号化コンテンツKc[C]を得る。この暗号化コンテンツKc[C]は、コンテンツ記録部208に渡され、ターゲット側のメディアに記録される(ステップS263)。

【0127】一方、コンテンツ復号鍵Kcは、一端、制御部205aに渡された後、ライセンス生成部205cに渡される。ライセンス生成部205cでは、メディアID取得部206からターゲット側のメディアのメディアID(MID)を取得し(ステップS256)、 $w=f(MID)$ によりライセンス鍵wを作成する(ステップS257)。

【0128】また、デジタルライセンス情報に含まれるコンテンツ利用条件Uを複製形態情報Qの利用条件情報を参照し、私的複製コンテンツに認められた範囲で決定する(ステップS258)。

【0129】次に、コンテンツ鍵Kcと利用条件Uとから認証子(MAC)を生成する(ステップS259)。これによってデジタルライセンス情報Loを生成し(ス

テップS260)、先に生成したライセンス鍵wを使ってデジタルライセンス情報を暗号化して、暗号化デジタルライセンス情報Lを得る(ステップS261)。

【0130】得られた暗号化デジタルライセンス情報Lをライセンス記録部207によってターゲット側のメディアに記録する(ステップS262)。

【0131】以上で、コンテンツ記録装置の説明を終える。

【0132】次に、上記第2の実施形態のいくつかの変形例(第3～第6の実施形態)について述べる。

【0133】(第3の実施形態)オリジナルコンテンツ以外(とくに公的複製コンテンツ)を複製する際には、私的複製コンテンツ作成部204では、当該コンテンツを適度に劣化させることが望ましい。これは劣化によって複製への期待が薄れ、正式な販路にのった公的複製コンテンツの販売が促進されるからである。この意味でアナログライセンス情報検出修正部204fにおいてコンテンツにノイズを載せるかデータ圧縮における圧縮率を上げるかによってこれを実現する構成も考えられる。このためにはデータ圧縮部204hの圧縮率を調整して劣化が起こる程度にする方法もしくはアナログライセンス情報を埋め込む際に埋め込みを極端にしてコンテンツの劣化がおこる程度までにする方法が考えられる。特に後者の場合、アナログライセンス情報が剥離させにくくなるというメリットもある。

【0134】(第4の実施形態)コンテンツの種類としてオリジナルコンテンツを認めない記録装置(もしくは記録再生装置)も考えられる。このような装置は、例えば、図21の構成において、オリジナルコンテンツ作成部205を省き、上記説明のうち、オリジナルコンテンツの入力およびオリジナルコンテンツでの複製に関する処理を省けばよい。

【0135】逆に、少なくともオリジナルコンテンツの入力を認める場合、オリジナルコンテンツとして認める入力端子を限定する方法が考えられる。この方法によれば、例えば、マイク端子から入力される音声はオリジナルコンテンツとして記録できるが、ラジオ端子から入力される音声は私的複製コンテンツとして記録させるような機構を取ると、入力媒体によって複製コンテンツの種類を決定することができ、例えば本記録装置のフォーマットで入力されていなくても記録することができるばかりか、当該複製がオリジナルコンテンツからのものなのかそうでないのかを区別することができる。

【0136】(第5の実施形態)第1の実施形態のコンテンツ再生装置と第2の実施形態のコンテンツ記録装置はそれぞれ独立の機構を有しているが、一体化した形態の記録再生装置を考えることも可能である。この場合、同じ機能を持つ構成要素であるメディアID取得部、データ圧縮部、データ解凍部などを共通化することも可能である。

【0137】（第6の実施形態）記録されるソースコンテンツをアナログのみに限り、私的複製コンテンツへの複製しか許さないという形態も存在する。このようにすることによって、デジタルコンテンツを記録する際、一端アナログレイヤを経由することによって、コンテンツの質的劣化を引き起こすことができ、従来の私的複製と同程度の質的劣化が実現され、コンテンツの質の上での私的複製が実現できる。

【0138】このようなコンテンツ記録装置の構成を図32に、その処理の流れを図33～図34に示す。

【0139】以下、図32のコンテンツ記録装置について、図33～図34に示すフローチャートを参照して説明する。

【0140】コンテンツ入力部301からアナログコンテンツCaが入力される（ステップS301）。入力されたアナログコンテンツCaは、アナログライセンス情報検出修正部302に送られ、そこでアナログライセンス情報が抽出され（ステップS302）、アナログライセンス情報に含まれるコピー回数制限が「1」以上であることを確認する（ステップS303）。そうでなかった場合はこれ以上複製は生成できないのでエラー出力する（ステップS304）。

【0141】以下、アナログライセンス情報が存在しないか、コピー回数制限が「1」以上であるとする。アナログライセンス情報がない場合、コピー回数制限は私的複製コンテンツの上限値に設定し、あった場合はコピー回数制限を「1」減じ、いずれの場合も複製情報を私的複製コンテンツに設定したアナログライセンス情報を作成し、アナログライセンス情報が既に存在する場合はそれを取り除いた後、新たに作成されたアナログライセンス情報をコンテンツに埋め込む（ステップS305～ステップS306）。

【0142】アナログライセンス情報が埋め込まれたコンテンツCaはA/D変換部303に送られ、デジタルコンテンツCdに変換する（ステップS307）。デジタルコンテンツCdは、データ圧縮部305に送られ、圧縮されたコンテンツCを作成する（ステップS308）。

【0143】コンテンツCは、全体制御部304を経由してコンテンツ暗号化部307へ送られ、コンテンツ暗号化部307では、コンテンツ鍵生成部309で生成されたコンテンツ復号鍵Kcを使って、コンテンツCを暗号化し、暗号化コンテンツKc[C]を作成する（ステップS309～ステップS310）。

【0144】コンテンツ暗号化部307は、一方でコンテンツ復号鍵Kcを全体制御部304に送り、全体制御部304が決める利用条件Uとともにライセンス生成部306に送る。

【0145】ライセンス生成部306では、コンテンツ復号鍵Kcと利用条件Uから認証子（MAC）を生成

し、デジタルライセンス情報Loを作成する。生成されたデジタルライセンス情報Loは、ライセンス暗号化部308に送られ、ライセンス暗号化部308ではライセンス鍵生成部310で生成されたライセンス鍵wを使ってデジタルライセンス情報Loを暗号化する（ステップS311～ステップS314）。

【0146】ここで、ライセンス鍵生成部310の処理の流れを説明する。ライセンス鍵生成部310では、メディアID取得部312を経由して暗号化コンテンツを記録するメディアのメディアID（MID）を取得し（ステップS312）、

$w = f(MID)$

により、ライセンス鍵wを生成する（ステップS313）。

【0147】さて、暗号化デジタルライセンスLは、ライセンス記録部311を経て、メディアに記録される（ステップS315）。同様に、暗号化コンテンツKc[C]もメディアに記録される（ステップS316）。

【0148】第1の実施形態でも述べたオリジナルコンテンツを許さない再生装置を本実施形態の記録装置と一体化するか、もしくは対として使うことによって、よりセキュリティの高いコンテンツ記録再生装置が作成できる。即ち、本発明の記録再生装置以外からのコンテンツを入力して記録する際にはアナログ入力しか認められず、デジタルコンテンツの記録には私的複製コンテンツに制限されるからである。このことは即ち、デジタルでの記録再生の世界であっても一端アナログを経由するため、従来からの記録再生システム以上の品質向上は望めないことを意味しており、複製の抑止力となると同時に公的複製コンテンツの価値を相対的に上げ、公的複製コンテンツの販売市場を確保することがより確実にできる。

【0149】（第7の実施形態）本実施形態では、デジタルコンテンツを購入再生する際に利用するコンテンツ販売装置とコンテンツ購入装置について説明する。ここでは、例えば、デジタルコンテンツをインターネットサーバ或は自動販売機経由で購入／販売する仕組みの一形態を示す。

【0150】まず、コンテンツ販売装置の実施形態を説明する。コンテンツ販売装置とは購入要求に応じて公的複製コンテンツを作成し、販売する販売装置を言う。本実施形態では、ネットワーク上に実現された電子商店が開設するコンテンツ販売サーバ装置を想定している。

【0151】図35は販売サーバの全体構成図、図36は、図35中のライセンス生成部403の構成図である。

【0152】まず、販売サーバの全体の処理の流れを示す図37と図38を参照して説明する。

【0153】販売サーバはクライアントからのコンテンツ購入要求を受信することによって動作を開始する（ス

テップS401)。購入要求情報は図39に示すように、購入申込をした顧客のID情報と、購入したいコンテンツのコンテンツID(CID)、購入利用条件、

(Uc)、顧客がコンテンツを記録する記録メディアのメディアID(MID)、クライアントアドレスからなっている。

【0154】販売サーバは、購入要求情報を受信すると、これを全体制御部402へ送り、購入要求情報に含まれているコンテンツIDをコンテンツ検索部405に送り、コンテンツデータベース(DB)407を検索して、コンテンツ復号鍵Kcと販売金額P(と場合によっては、暗号化コンテンツKc[C])を抽出する(ステップS402)。

【0155】ここで、暗号化コンテンツKc[C]を取り出す条件として、例えばコンテンツIDが十分大きなビット数で表現されており、冗長なビットが存在するならば冗長ビットのうちの1ビットを暗号化コンテンツを送信するか否かの判別フラグとすることができる。

【0156】次に(もしくはコンテンツ検索部405における処理と同時に)、全体制御部402は、顧客IDをキーに顧客のクレジット番号を顧客データベース(DB)408から検索し、検索されたクレジット番号で信用照会を行なう(ステップS403ステップS404)。信用照会の結果支払が可能ならば、以下で詳しく述べる手順に従って暗号化デジタルライセンス情報を生成し、暗号化デジタルライセンス情報をクライアントのアドレスに出力する(ステップS405～ステップS407)。信用照会の結果支払が不可能である場合は、その旨クライアントのアドレスへ通知する。通知及び出力は電子メールによっても良いし、直接ネットワーク接続されている場合には、接続されているネットワークを使えば良い。

【0157】次に、図36のライセンス生成部403の暗号化デジタルライセンス情報の生成処理について、図38に示すフローチャートを参照して説明する。

【0158】ライセンス生成部403は、コンテンツDB407から出力されたコンテンツ復号鍵Kcと購入要求情報から抽出されたメディアID(MID)との入力を受けて処理を開始する(ステップS411)。

【0159】まず、ライセンス生成部403内の制御部403bによって入力された利用条件Uを決定し、コンテンツ復号鍵Kcと利用条件Uから認証子(MAC)を生成して、デジタルライセンス情報Loを作成する(ステップS412～ステップS413)。

【0160】次に、入力されたメディアID(MID)より

$w = f(MID)$

によってライセンス鍵wを生成する(ステップS414)。ライセンス鍵生成部403cは、ライセンス鍵wとデジタルライセンス情報Loを制御部403bに送

り、制御部403bでは、ライセンス情報Loを暗号化することによって暗号化デジタルライセンス情報を生成する(ステップS415～ステップS416)。

【0161】さらに、サーバ秘密鍵データベース(DB)409から鍵サーバ秘密鍵Ksと、その秘密鍵のID(KID)を抽出し(ステップS417)、暗号化ライセンス情報Lに秘密鍵Ksでデジタル署名を施し(ステップS418)、これを付加して暗号化ライセンスLを作成する。そして作成されたデジタルライセンス情報Lを出力して処理を終える(ステップS419)。

【0162】ここで、デジタル署名の作成は公開鍵暗号で行ない、図6と図7に示すデータを作成する。デジタル署名ヘッダに含まれるデジタル署名全体長には当該ヘッダを含むデジタル署名の長さを、署名の種類には署名方式の種類の識別子を、署名検証鍵番号には秘密鍵のID(KID)をそれぞれ入力する。

【0163】以上で、コンテンツ販売装置、すなわち、販売サーバの説明を終了し、次に、販売に対応したコンテンツ購入装置の仕組みを説明する。コンテンツ購入装置は再生装置そのもののこともあるが、必ずしもその必要はなく、ネットワーク接続できるパーソナルコンピュータなどの機器や専用の装置であっても良い。

【0164】図40にコンテンツ購入装置の構成を示し、以下、図41～図42に示すフローチャートを参照して、コンテンツ購入装置について説明する。

【0165】コンテンツ購入装置には、コンテンツ選択インタフェース(IF)501を通じて、購入するコンテンツのコンテンツIDが入力され、全体制御部502に送られる(ステップS501)。コンテンツ選択IF501は、コンテンツIDをキーボードから入力する形式でも良いし、専用の検索ソフトか入力ソフトにより、ユーザが歌手名や作曲者などをキーに検索し、指定することによって入力しても良い。

【0166】全体制御部502では、コンテンツIDの入力を受けて、メディアID抽出部504を経由して当該コンテンツを記録する(もしくは既に記録されている)メディアからメディアID(MID)を抽出する(ステップS502)。

【0167】次に(もしくは同時に)、顧客情報保持部505から(購入者の)顧客ID、顧客アドレスを抽出し(ステップS503)、これら抽出された情報を基に図39に示すような購入要求情報を販売サーバに送信する(ステップS504～ステップS505)。

【0168】なお、本実施形態では、顧客情報は顧客情報保持部505に格納されているが、この部分を外部からの入力に変えても同様の処理ができる。

【0169】また、購入要求情報に従ってコンテンツ販売装置から暗号化ライセンスL(コンテンツ購入装置側に暗号化コンテンツがない場合は暗号化コンテンツKc[C]と共に)に送信されてきた時、コンテンツ販売装

置はこれらをメディアIDを抽出したメディアに記録する（ステップS511～ステップS512）。

【0170】以上で、コンテンツ購入装置の構成と処理の流れの説明を終了する。以上の構成からコンテンツ購入装置はコンテンツ再生装置と一体化ができることが分かる。即ち、図8に示した再生装置の構成は図40に示した販売クライアントの構成と機能的に独立であり、両方の機能を備えた装置が構成できる。同様に第2の実施形態で述べたコンテンツ記録再生装置との間にも同じ関係が成り立つ。

【0171】このため、コンテンツ販売装置とコンテンツ購入装置を一体化させたシステムも考えられる。これは、コンテンツ情報の自動販売機のような装置であり、図35のコンテンツ販売装置の構成にける課金部404を自動販売機における硬貨／紙幣検出格納装置とし、作成された暗号化ライセンスL（及び暗号化コンテンツ）を図40のコンテンツ購入装置の構成におけるメディア記録部503を経由してメディアに記録するようにすれば実現できる。

【0172】このような自動販売機を実現することにより、顧客はメディアを自動販売機に持参してコンテンツ及びライセンスを購入することができる。勿論、コンテンツ購入装置単独でも自動販売機を構成できる。その場合は電話回線等によってコンテンツ販売装置に接続されなければならない。

【0173】

【発明の効果】以上説明したように、本発明によれば、正当な経路で複製されたコンテンツ（公的複製コンテンツ）が、正当な権限なく複製されたコンテンツよりも有利な形態で流通可能となる。その結果、公的複製コンテンツの需要を増やし、コンテンツ供給者、コンテンツ利用者、電子機器供給者に利害にかなった情報流通機構を提供できる。

【図面の簡単な説明】

【図1】デジタルライセンス情報のデータ構成の一例を示した図。

【図2】暗号化デジタルライセンス情報のデータ構成の一例を示した図。

【図3】ライセンスヘッダのデータ構成の一例を示した図。

【図4】コンテンツ利用条件のデータ構成の一例を示した図。

【図5】アナログライセンス情報のデータ構成の一例を示した図。

【図6】デジタル署名のデータ構成の一例を示した図。

【図7】デジタル署名ヘッダのデータ構成の一例を示した図。

【図8】コンテンツ再生装置の構成例を示した図。

【図9】オリジナルコンテンツ再生部の構成例を示した図。

【図10】私的複製コンテンツ再生部の構成例を示した図。

【図11】公的複製コンテンツ再生部の構成例を示した図。

【図12】図8のコンテンツ再生装置の処理動作を説明するためのフローチャート。

【図13】オリジナルコンテンツ再生処理動作を説明するためのフローチャート。

10 【図14】私的複製コンテンツ再生処理動作を説明するためのフローチャート。

【図15】公的複製コンテンツ再生処理動作を説明するためのフローチャート。

【図16】暗号化コンテンツ復号部の構成例を示した図。

【図17】暗号化ライセンス復号部の構成例を示した図。

【図18】暗号化コンテンツ復号処理動作を説明するためのフローチャート。

20 【図19】暗号化ライセンス復号処理動作を説明するためのフローチャート。

【図20】暗号化デジタルライセンス情報の他の例を示した図で、デジタル署名を用いない場合を示したものである。

【図21】コンテンツ記録装置の構成例を示した図。

【図22】私的複製コンテンツ作成部の構成例を示した図。

【図23】オリジナルコンテンツ作成部の構成例を示した図。

30 【図24】図21のコンテンツ記録装置の処理動作を説明するためのフローチャート。

【図25】私的複製コンテンツ作成処理動作を説明するためのフローチャート。

【図26】私的複製コンテンツ作成処理動作を説明するためのフローチャート。

【図27】オリジナルコンテンツ作成処理動作を説明するためのフローチャート。

【図28】オリジナルコンテンツ作成処理動作を説明するためのフローチャート。

40 【図29】オリジナルコンテンツ作成処理動作を説明するためのフローチャート。

【図30】複製形態情報のデータ構成の一例を示した図。

【図31】複製形態情報中の利用条件情報のデータ構成の一例を示した図。

【図32】コンテンツ記録装置の他の構成例を示したもので、記録するコンテンツがアナログ信号の場合を示したものである。

【図33】図32のコンテンツ記録装置の処理動作を説明するためのフローチャート。

50 【図34】図32のコンテンツ記録装置の処理動作を説

明するためのフローチャート。

【図35】コンテンツ販売装置（販売サーバ）の構成例を示した図。

【図36】図35のコンテンツ販売装置のライセンス生成部の構成例を示した図。

【図37】図35のコンテンツ販売装置の処理動作を説明するためのフローチャート。

【図38】ライセンス生成処理動作を説明するためのフローチャート。

【図39】購入要求情報のデータ構成の一例を示した図。

【図40】コンテンツ購入装置の構成例を示した図。

【図41】図40のコンテンツ購入装置の処理動作を説明するためのフローチャート。

【図42】図40のコンテンツ購入装置の処理動作を説明するためのフローチャート。

【符号の説明】

（コンテンツ再生装置）

- 1…全体制御部
- 2…コンテンツ入力部
- 3…再生インタフェース（I/F）部
- 4…私的複製コンテンツ再生部
- 5…公的複製コンテンツ再生部
- 6…オリジナルコンテンツ再生部
- 7…デジタル出力部
- 8…アナログ出力部

【図1】

デジタルライセンス情報 L。

ライセンス ヘッダ (LH)	コンテンツID (KID)	コンテンツ 利用条件 (U)	暗証子 (MAC)	デジタル署名
----------------------	------------------	----------------------	--------------	--------

【図3】

ライセンスヘッダ LH

ライセンス情報の長さ	コンテンツID	複製情報	コンテンツIDの長さ
------------	---------	------	------------

【図5】

アナログライセンス情報 L

コピー回数制限情報	複製情報
-----------	------

デジタル署名

デジタル署名ヘッダ	デジタル署名
-----------	--------

【図6】

（コンテンツ記録装置）

- 201…全体制御部
- 202…コンテンツ入力部
- 203…記録インタフェース（I/F）部
- 204…私的複製コンテンツ作成部
- 205…オリジナルコンテンツ作成部
- 206…メディアID取得部
- 207…ライセンス記録部
- 208…コンテンツ記録部

（コンテンツ販売装置）

- 401…コンテンツ購入受付部
- 402…全体制御部
- 403…ライセンス生成部
- 404…課金部
- 405…コンテンツ検索部
- 406…出力部
- 407…コンテンツデータベース（DB）
- 408…顧客データベース（DB）
- 409…サーバ秘密鍵データベース（DB）

20 （コンテンツ購入装置）

- 501…コンテンツ選択インタフェース（I/F）
- 502…全体制御部
- 503…メディア記録部
- 504…メディアID抽出部
- 505…顧客情報保持部
- 506…コンテンツ入力部

【図2】

番号化デジタルライセンス情報 L

ライセンス ヘッダ (LH)	コンテンツID (KID)	コンテンツ 利用条件 (U)	暗証子	デジタル署名
----------------------	------------------	----------------------	-----	--------

【図4】

コンテンツ利用条件 (U)

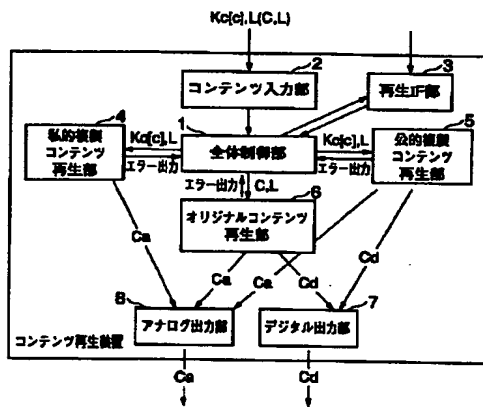
デジタル出力フラグ (Fo)	有効期限情報	有効回数情報
-------------------	--------	--------

【図7】

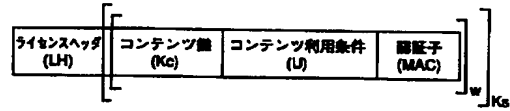
デジタル署名ヘッダ

デジタル署名 全体長	署名の種類	署名検証番号
---------------	-------	--------

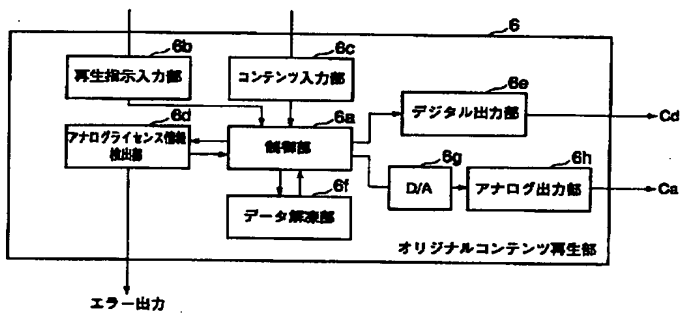
【図8】



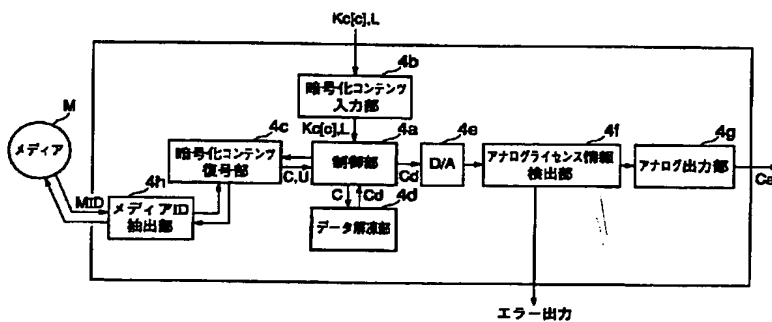
【図20】



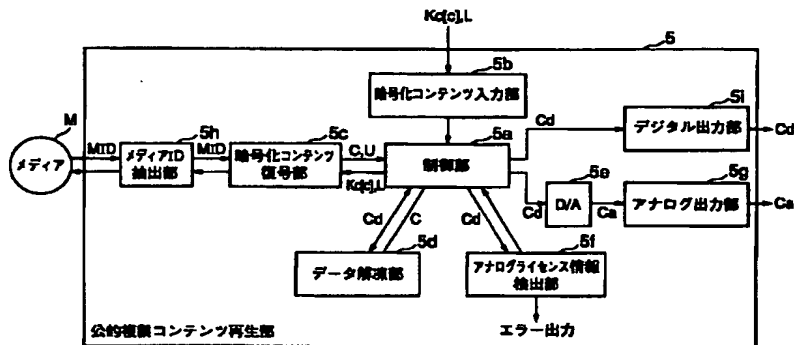
【図9】



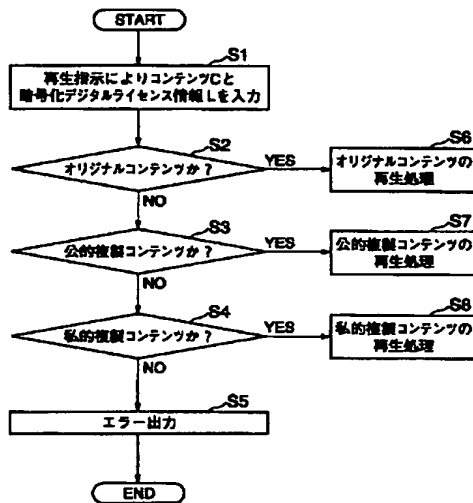
【図10】



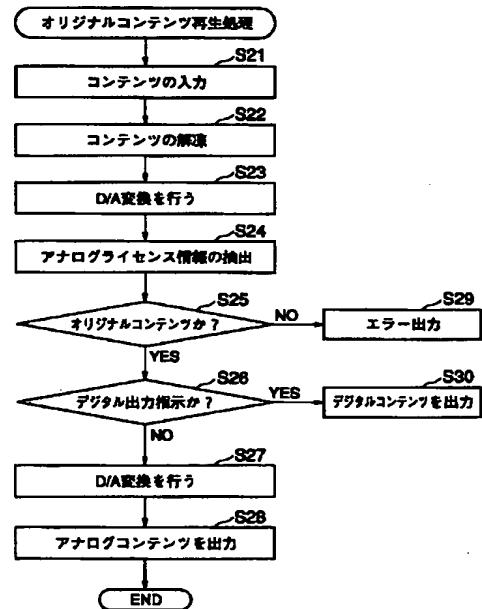
【図11】



【図12】



【図13】



【図29】

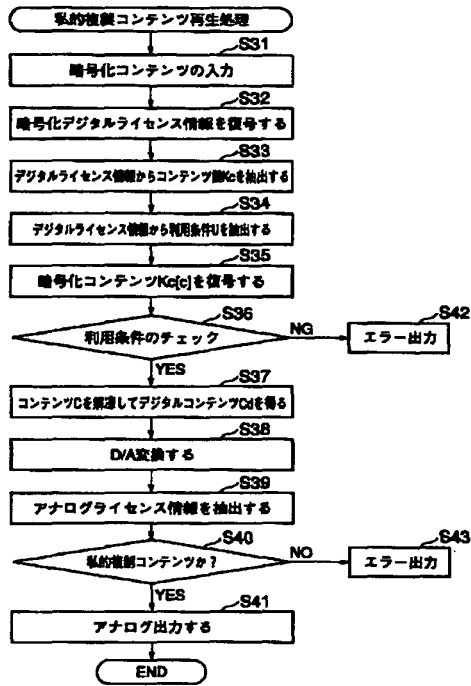


【図30】

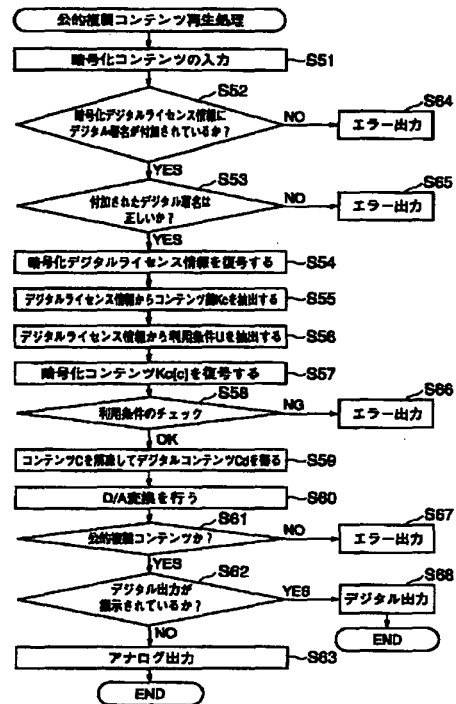
複製形態情報Q

複製コンテンツの種類	複製利用条件情報
------------	----------

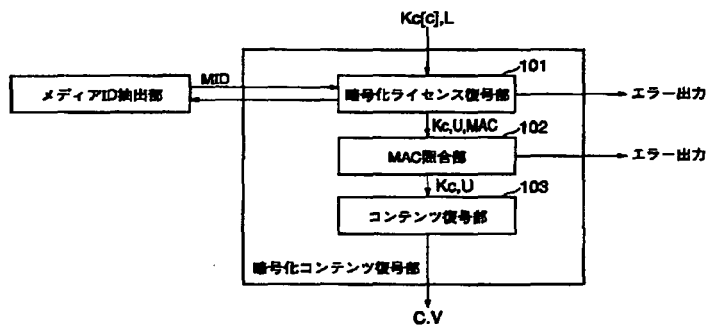
【図14】



【図15】



【図16】

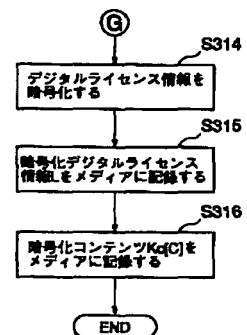


【図31】

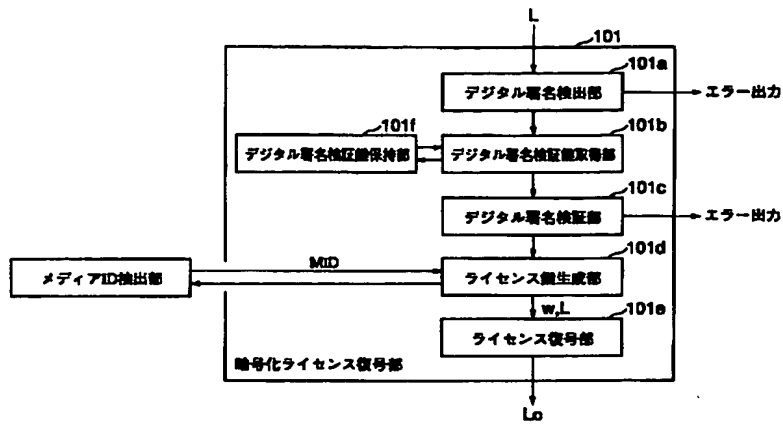
利用条件情報

デジタル出力 フラグ(Fa)	有効期限情報	有効利用回数情報	コピー回数制限 情報
-------------------	--------	----------	---------------

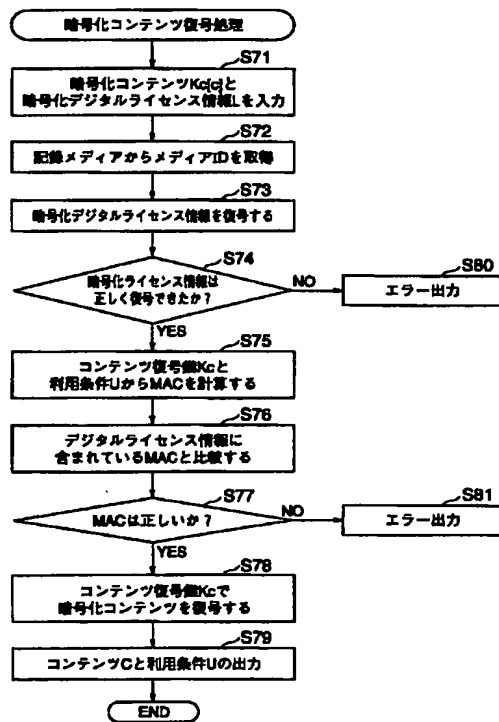
【図34】



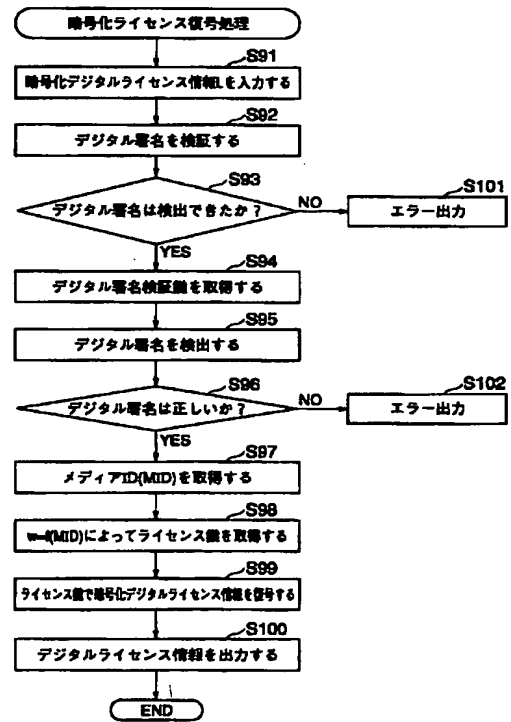
【図17】



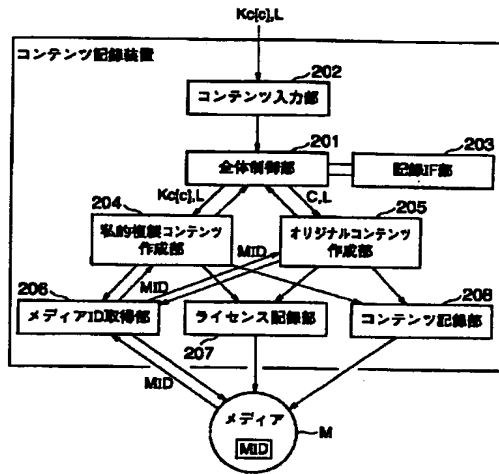
【図18】



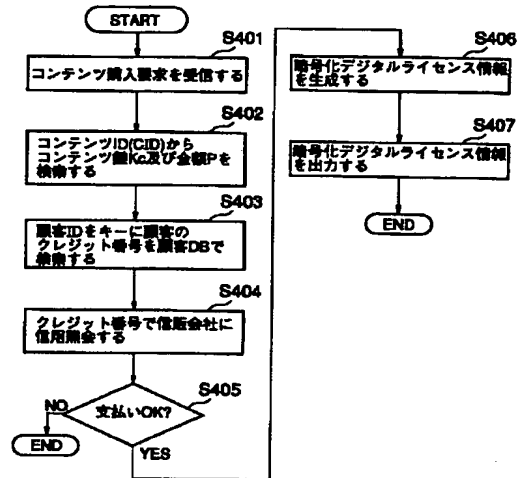
【図19】



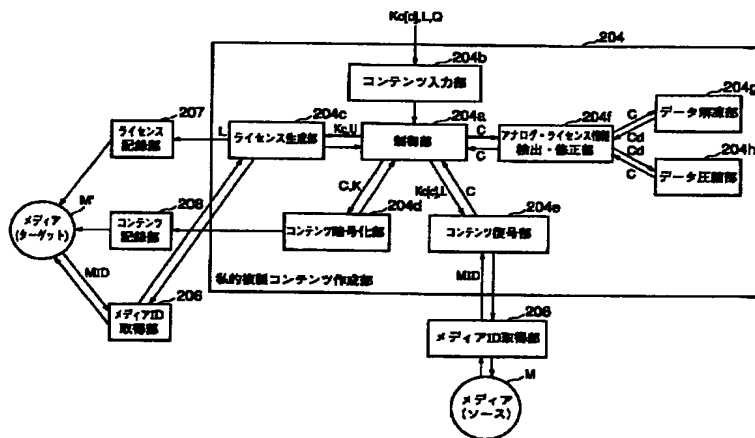
【図21】



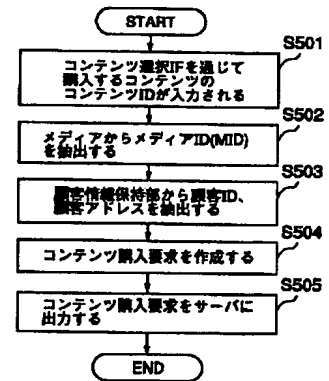
【図37】



【図22】



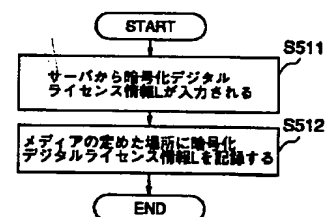
【図41】



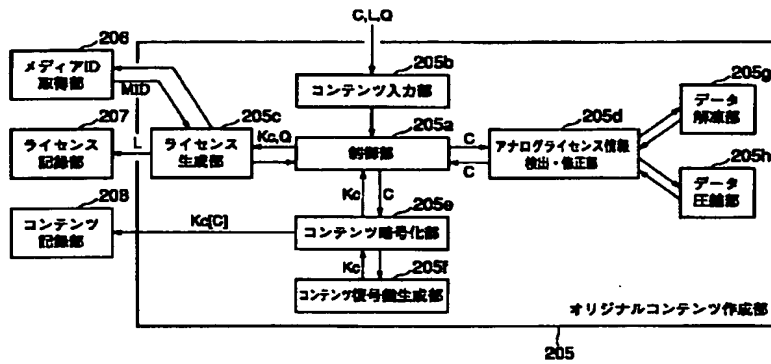
【図39】

顧客ID	コンテンツID (CID)	購入利用条件Uc	メディアID (MID)	クライアントアドレス
------	---------------	----------	--------------	------------

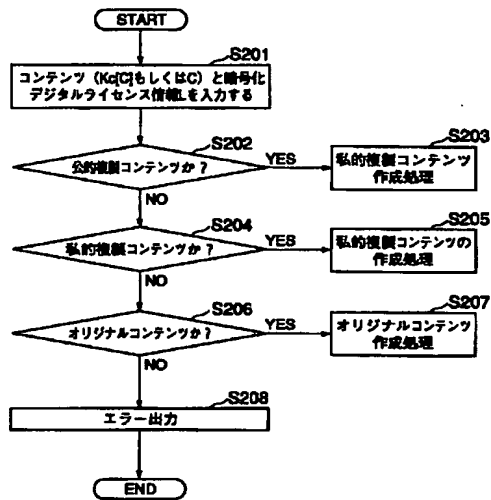
【図42】



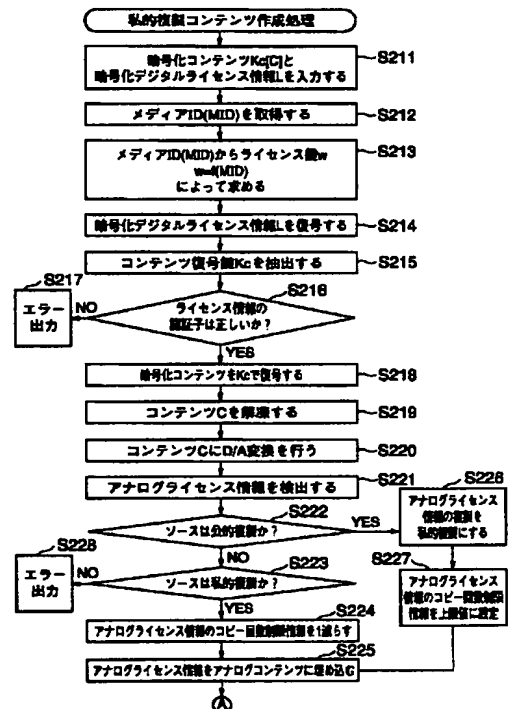
【図23】



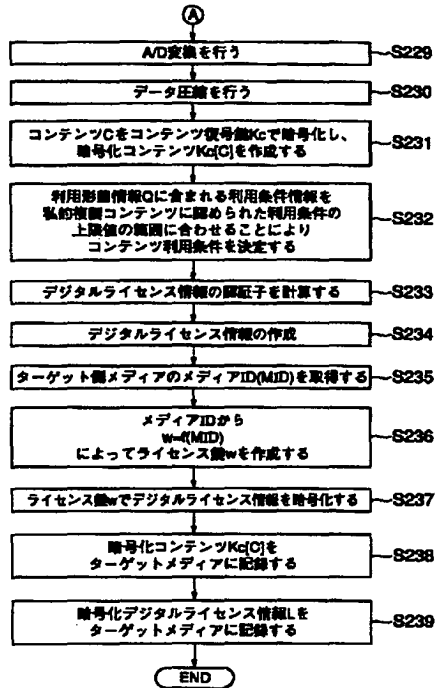
【図24】



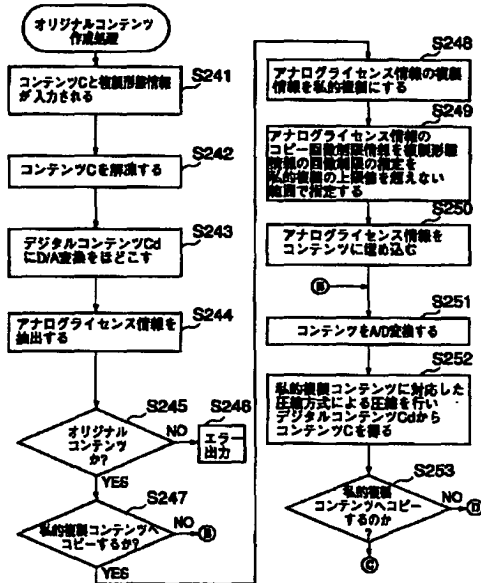
【図25】



【図26】

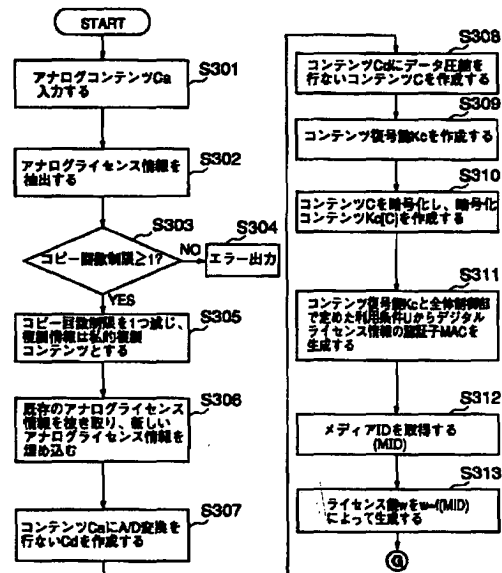
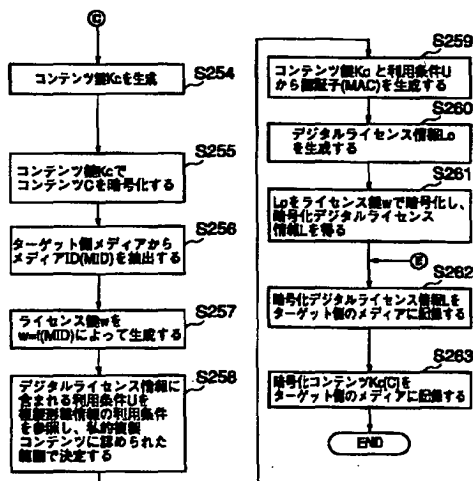


【図27】



【図33】

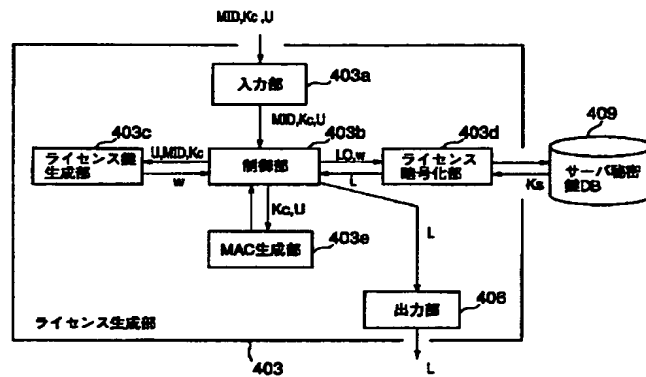
【図28】



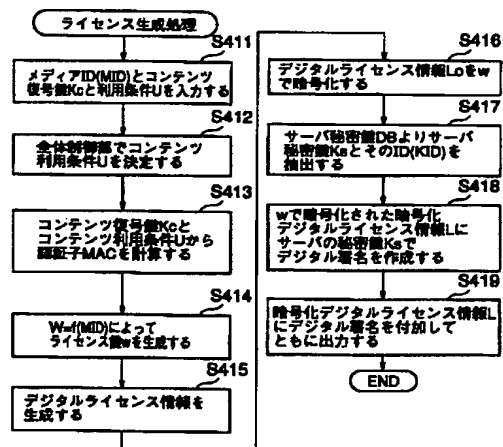
[illegible]

The diagram illustrates the architecture of a content distribution system. At the top, an arrow labeled '購入要求情報' (Purchase Request Information) points to the 'コンテンツ購入受付部' (Content Purchase Reception Unit) 401. This unit sends 'MID, CID, Lb' to the '金銭制御部' (Financial Control Unit) 402. The '金銭制御部' 402 is connected to several other components: it sends 'L' to the 'ライセンス生成部' (License Generation Unit) 403; it sends 'CID' to the 'コンテンツ検索部' (Content Search Unit) 405; it sends 'D1' to the '課金部' (Billing Unit) 404; and it sends 'P' to the 'サーバ秘密照会DB' (Server Secret Inquiry DB) 409. The 'ライセンス生成部' 403 sends 'U, MID, Kc' to the '金銭制御部' 402. The 'コンテンツ検索部' 405 sends 'Kc, P(Kc, [C])' to the '金銭制御部' 402 and 'L(Kc, [C])' to the '出力部' (Output Unit) 406. The '出力部' 406 sends 'Kc, P(Kc, [C])' to the 'コンテンツDB' (Content DB) 407. The '課金部' 404 is connected to the '顧客DB' (Customer DB) 408. The 'サーバ秘密照会DB' 409 and the 'コンテンツDB' 407 are represented by cylinder icons.

【図36】



【図38】



[illegible]

(72)発明者 半田 豊
神奈川県川崎市幸区小向東芝町1番地 株
式会社東芝研究開発センター内

(72)発明者 大盛 善啓
神奈川県川崎市幸区小向東芝町1番地 株
式会社東芝研究開発センター内
Fターム(参考) 5D044 DE17 DE48 DE49 EF05 FG18
GK12 GK17 HH15 HL07

